Department of the Army
First Region (ROTC)
United States Army Cadet Command
Fort Bragg, NC 28307-5000

FRMOI 380-3
22 February 2002

Security

INFORMATION SYSTEMS SECURITY - MANAGERS GUIDE

FOR THE COMMANDER:

KERRY R. PARKER
COL, AD
Chief of Staff

PROPONENT: The proponent of this publication is Information Management Division, Headquarters, First Region (ROTC), US Army Cadet Command. Comments should be sent directly to Headquarters, First Region (ROTC), US Army Cadet Command, ATTN: ATOA-IM, Fort Bragg, North Carolina 28307-5000.

SUPERSESSION: This FRMOI supersedes FRMOI 380-3, 24 Nov 00.

DISTRIBUTION: A; D; J; S
Distribution codes used are explained in FRMOI 25-1.

This document is available on the First Region (ROTC Web site at:
www.rotc1.bragg.army.mil

FOREWORD

Few things have impacted today's Army more than technological advancements and the revolution in computers has been foremost of these advances.

From desktop or portable microcomputers to giant supercomputers, automated information systems are everywhere. These systems perform critical combat development, logistic, personnel, financial, medical, and other functions that sustain and maintain forces during peacetime, mobilization, and war.

Army information systems and the data processed on them are quite valuable - and quite vulnerable. Since we rely on these assets (and assets they truly are), their protection is crucial.

We can achieve that protection through prudent computer security measures. Although information systems security is a well established field, it often hasn't received the support it needs from all levels of command and management. This support is vital. Without it, no security program can succeed.

This FRMOI was written to help inform you about the need for and benefits of security for your vital information processing systems. You'll be shown some of the most common security problem areas and given some recommended counter-measures for these problems.

This FRMOI doesn't tell you exactly what to do to safeguard your systems. You won't be given a recipe for surefire control and protection for all information systems. That simply isn't possible. Each operation is different and needs a unique set of controls and safeguards.

Each information system also needs active security management. Security isn't something you do once and then forget. Effective security requires ongoing commitment and effort.

Like any operation, security of information systems requires your involvement, imagination, and decisiveness. Perhaps with a combination of the ideas in this publication and your own leadership and management skills, you'll avoid the serious problems - or even disasters - that accompany some automated operations.

INTRODUCTION

It's been said there is no such thing as complete security, only degrees of insecurity.

Truly, uncertainty is a part of each of our lives. Whether we realize it or not, the unknown and unexpected await us at every turn. Regardless of our endeavor, unforeseeable factors dog us.

Information systems security efforts are no different from any other part of our lives. The closest we could come to a completely secure computer system would be to place it in a bomb, fire, earthquake, and flood-proof enclosure and remove all power and communications links. Of course, such a system would be unusable, but it would be quite secure.

Short of that, what can you do to help secure your computer systems?

YOU CAN DO A LOT!

As you'll see, there are many practical and effective safeguards for your information processing assets. The situation isn't hopeless.

Perhaps the first step is to see computers for what they are. A computer is just a tool, not a device that will "auto-magically" solve your problems. Powerful as it may be, you must treat a computer as you would any other tool. You must apply it to the proper job (a hammer makes a poor screwdriver, and vice versa). You must use it carefully and responsibly.

The daunting combination of newness, power, and complexity can cause many problems with information systems. It's easy to become so enthralled with efficiency and performance increases that you overlook crucial controls and safeguards.

You are responsible for the computer systems used in your organization. Even though you may not know as much about computers as you'd like, it's your duty to effectively manage and protect the systems entrusted to you. It's a weighty and difficult responsibility - one you can't delegate to others.

It is time to begin asking the truly important questions about your present and future information systems. Not simply "how fast?" or "how big?" or "how powerful?", but also "how do I control and safeguard?" Although protection of information and computers is often perceived as a specialized security issue, the overall concern is your responsibility.

WHY SHOULD I BE CONCERNED?

"Security is just another headache, and I already have enough headaches." "Controls are strictly overhead - they offer no return on investment." "Security is simply a hindrance to accomplishing our mission." "I don't need to worry about computer security - I don't process classified data."

Sound familiar? Have you expressed these or similar ideas? Maybe we better look at the situation a little more closely.

THE VALUE OF INFORMATION

Information is a unique asset. It is intangible, so its value may be difficult or impossible to measure. Information can be stolen yet not missed. It can be transformed without your knowledge. Information may seem to be only a by-product of what you do but may in fact be the most valuable part of your work. Much of the information with which the Army works could greatly aid our adversaries and competitors.

Financial and logistics information, personnel files, For Official Use Only (FOUO) data, contractual records, and similar data need safeguarding. Loss or misuse of such information could cause serious damage or embarrassment to your operations.

Even seemingly nonsensitive computerized data must be protected from unauthorized modification or destruction. After all, if the data is worthless, what is it doing on a computer? The very fact that data is important enough to collect, process, communicate, and store, shows that it has a degree of value.

DECISION MAKING DEPENDS ON DATA INTEGRITY

Data integrity - the accuracy, completeness, and timeliness of the data is crucial. Decisions can only be as sound as the information used in making them.

You feed your computer system vast quantities of data. You manipulate that data or extract portions of it to get the specific information you need. Then you act on that information; you make decisions and develop plans. You rely upon that information implicitly.

But how accurate is that information? Do you ever really question its correctness and completeness, or do you assume "if the computer says so, it must be true?"

You may have heard the expression "garbage in, garbage out." This means if the data you put in your computers is worthless, then you can't expect anything worthwhile out of them. Yet unless the output is obviously - glaringly - wrong, we often don't question its accuracy or completeness. Although it may be "garbage" in, we treat it as "gospel" out.

If information is erroneous, incomplete, or untimely, mismanagement is the result. That isn't the only cause of mismanagement, of course. But no matter how talented you are, you will fail if you base your decisions upon false premises.

WHAT ABOUT COMPUTER CRIME?

You must safeguard against more than simple errors and omissions. An American Bar Association survey showed that 40 percent of the respondents had computer crime or abuse incidents within the year preceding the survey. Total losses amounted to hundreds of millions of dollars. Even that only hints at the true cost since many organizations are either unaware of the occurrence of a security breach or may refuse to admit anything that could create negative publicity for them.

The Army is vulnerable to many of these same damages. In addition to such business considerations, we must guard against espionage and sabotage. The cost to the Army and the nation if sensitive or classified information is compromised or vital operations disrupted could be enormous.

Computer crime and abuse is like costly termite infestation; by the time you discover the problem, the damage may already be extensive.

THE VALUE OF SECURITY

Protective measures can seem expensive, but they are needed to prevent even greater loss. Such measures can prove to be excellent ways of reducing overall costs. While some procedural safeguards are a slight hindrance to getting the job done, they are necessary to maintain a degree of control. After all, our concern should be overall effectiveness, not just efficiency.

You can't afford to look upon protective measures as "stumbling blocks" in the way of doing your primary job. Security practices must be seen for what they are - measures necessary to prevent greater losses from potential risks. Security measures may slow things down a little or be inconvenient at times, but without them, the consequences could be severe.

WHAT MAKES A SUCCESSFUL OPERATION?

Success is measured by many factors, not just speed or volume. We can make an analogy between computer security and the everyday situation of driving your car.

Your goal or mission might be to drive to a particular nearby destination. If your only concern were accomplishing that goal without inefficiency or delay, you'd drive as fast as your car can go. You'd ignore speed limits, traffic signs and signals. You'd give no thought to

possible mechanical failure or other unexpected incidents. Too bad for anyone or anything that got in your way! You'd see all of those as "hindrances" and as things which "slow you down" as you try to reach your objective.

Clearly that approach to driving is intolerable. Yet how similar is your approach to your information processing systems?

Do you ignore security controls because they slow you down? Do you refuse to put controls in place because they hinder your operation? Do you fail to do even simple things, like making data backups, because it's inconvenient or you "don't have time"?

All information systems require some degree of control and protection. We have become so reliant upon our automated systems that it would be difficult - sometimes impossible - to do without them. Yet safeguarding these systems is an annoyingly complex problem, one that cannot be solved by gimmicks. There are no shortcuts.

COMPUTER SECURITY IS A MANAGEMENT PROBLEM

Despite its technical overtones, information systems security isn't primarily a technical problem, it's a managerial one. This simply can't be stressed strongly enough.

The technical means are available to counter virtually any threat to your automated operations. All that remains is to identify the specific problems and the degree of control needed, and then to have the fortitude to insist upon needed safeguards.

Security demands your involvement. You can't simply delegate all the responsibility to your security staff. Nor can you afford to wait for computer technology to slow down or for a perfectly secure computer system to become available.

THE BENEFITS OF GOOD COMPUTER SECURITY

Security measures may seem to offer nothing to help you get your job done - today that is. But effective management is much more than the production of immediate results. A short term view especially distorts the true value of safeguards.

By taking effective steps to protect your information systems resources, you will be more likely to avoid the delays, errors, and even disasters that plague some automated information systems. Taking a few extra moments to protect your system today helps to ensure your ability to do your job today, tomorrow, and for many more tomorrows. You will help ensure continued mission capabilities.

You'll also improve your decision making since you will reduce the likelihood of inaccurate or incomplete data. This will allow the Army and the United States to preserve our competitive edge.

Security also helps prevent loss and thus can lead to overall resource savings. By preventing fraud and computer-aided theft, you can more than offset the cost of security controls. By

safeguarding legally-protected material and eliminating individual piracy you can avoid costly lawsuits and fines.

Finally, you can avoid public embarrassment. Nobody wants to be spotlighted as a glaring example of how to poorly operate a computerized information system.

WHY TECHNICAL CONTROLS ALONE WON'T WORK

There is one simple reason for the above statement: computer security came after the computer.

Scientists' first goal was to achieve an operational capability. Army operations have taken the same approach. Get the system designed, built, and running. Few people seem to have anticipated the problems that computer security measures deal with. So technical safeguards are always at least one step behind operational capabilities.

A similar situation arose with the development of the automobile. Inventors were simply after a self-propelled land vehicle. They didn't anticipate, much less plan for, such important factors as traffic signals, rights-of-way, or speed limits. Some inventors didn't even plan for good brakes for their vehicle! They were so interested in making it go, they never put much thought to making it stop.

You probably installed your computer systems the same way. Your first and foremost concern was getting them operational to satisfy a particular mission requirement. Only later, perhaps only now, was the need for security measures apparent.

That's why technical controls alone are not enough. Security technology lags operational technology. This will hold true for most systems for the foreseeable future. Few computer systems are being designed with security controls in mind. Even then these controls are for the operating system software only. You still must plan and develop controls for specific applications.

Computer security measures must be multifaceted. Don't place too much reliance on any single safeguard.

And don't say you'll just wait until the security technology is available before you act. In all likelihood, it will never be enough.

AREAS OF CONCERN

The problems we face and the controls and safeguards needed are diverse.

As noted earlier, computers can be helpful tools, but to be effective you must manage them properly. Control measures must be an integral part of system operations throughout each system's life. Identify security concerns at the beginning of a project, develop safeguards as the project proceeds, and maintain security practices during operation. Even when a system's useful life is over, you must take care to dispose of equipment and data storage media properly to avoid compromising sensitive or classified data.

Just as lumber doesn't simply evolve from trees, information systems security doesn't evolve from system operation. You must have a plan and control measures must be inherent to that plan from the beginning.

As important and valuable as the computers themselves are, the data they process are usually even more so. So the security measures you apply to the computers should also be applied to the data, regardless of data location or format.

Even if the computer system you use isn't under your direct control, you are a "sponsor" of that system since it processes your data. You therefore have a right - indeed, a responsibility - to specify controls and safeguards for your data. Tell the system owner of your requirements and make certain that your data gets the needed protection.

THE THREE ASPECTS OF INFORMATION SYSTEMS SECURITY

We can divide our efforts to protect information resources into three broad areas: data confidentiality, data integrity, and data availability.

Data confidentiality means protecting the information from those who have no valid need for it. This is what comes to mind most quickly when someone mentions security.

We've already discussed data integrity, the accuracy, completeness, and timeliness of your information. Decision making and overall success hinge on data integrity.

Data availability refers to ensuring our capability to process and communicate information. Considerations include backups for processing systems, software, and data.

Safeguards in one of the above areas often aid one or both of the others. You will find that good security practices have a synergistic effect.

CONTROL MEASURES

Control measures used to protect your systems fall into several broad categories:

- Physical protection.

- Software security.

- Communications controls.

- Personnel security.

- Procedures.

- Contingency planning.

- Security awareness training.

- Security management.

Let's take a brief look at each.

PHYSICAL PROTECTION

Like other protective measures, physical security of information systems depends upon the type of system and the sensitivity of the data processed. The safeguards needed by a microcomputer are different from those needed by a mainframe computer. A word processing system needs different controls than one which processes financial information.

Physical security is achieved through an in-depth application of barriers and procedures, including key control, access control, structural standards, lighting, inventory, and accountability. Physical security also deals with such things as prevention, detection, and suppression of fires, temperature controls, water damage prevention, control and protection of supporting utilities, and protection from magnetism.

You must apply protective measures to the areas housing computer equipment, data storage media (tapes, diskettes, etc.), and hard copy output.

ACCESS CONTROL

One of the most important physical security measures is controlling access to the computer and all peripheral devices. If you strictly limit access to only authorized users, you will have gone far toward protecting the system and its data. Then if you do have a problem, the number of potential suspects is relatively small.

Unfortunately, strict access control often isn't practiced, especially in an office environment. This often leads to more problems than you might expect. An unauthorized user can unintentionally destroy or compromise valuable information simply by "playing" with an unattended system. Malicious intruders can do even worse.

Access controls offer effective yet usually inexpensive safeguards to your systems - if you will enforce them.

PHYSICAL SECURITY FOR OFFICE AUTOMATION

Physical security for mainframe systems usually requires careful and detailed planning coordinated with a security specialist. Those controls are beyond the scope of this document.

FOR AN OFFICE ENVIRONMENT, THE SAFEGUARDS NEEDED INCLUDE:

- fire protection, including smoke detectors, portable extinguishes, and building sprinkler systems.

- protection from flood and other water damage (leaking roofs and overhead pipes destroy a surprising number of computers and data storage media each year).

- environmental controls (such as prohibiting smoking, drinking, or eating around computer equipment or data storage media).

- protection from static electricity and power surges, and protection from magnetism (such as radio speakers, telephones, and paper clip holders).

PHYSICAL SECURITY FOR LAPTOP COMPUTERS

Physical protection of portable "laptop" computers presents many problems. These systems are designed to be routinely removed from the office and operated in unprotected surroundings. Airplanes, airports, hotel lobbies, conference rooms, and other places where these systems are used offer no access controls and only minimal physical safeguards. In these environments, use laptop systems only for small amounts of the least sensitive data. Carefully evaluate the convenience factors offered by these systems against the potential for data loss, corruption, or disclosure.

SOFTWARE SECURITY

The processing logic you apply to your data must be sound if the result is to be of value. This logic takes the form of operating systems and applications software (programs). You can achieve software integrity by preventing deliberate or inadvertent unauthorized manipulation of software.

SOFTWARE INTEGRITY

Software used to process sensitive information must have positive security attributes and capabilities. Don't use software known to contain inherent security weaknesses to process sensitive information without strong supplemental controls.

Operating systems as well as applications programs, whether specially developed or commercially procured, may contain serious errors. Even if the original versions are error free, you must take care when modifying software to be sure that it remains free of errors and unauthorized routines. Without good software controls, the result may be erroneous data or even fraud.

When you modify software, don't use it in a production mode until it's run against test data and results verified. Strictly control program modification so no one can make unauthorized changes.

Carefully document software to ensure its proper use and maintenance. Documentation should include a program description, sample input and output formats, and security requirements. Data and file names should be descriptive. Reflect all software changes in the documentation.

For microcomputers, a considerable number of special purpose public domain software packages are available at little or no cost. You must acquire such software with caution, however. Accept them only from recognized sources, not from public bulletin boards or similar uncontrolled sources. Before using them for production work, try them in a test environment. Check extensively for errors, peculiarities of use, and unexpected functions.

Make certain that all users know the importance or reporting anything out of the ordinary as they use various software. Errors or unauthorized program modifications are often discovered only by accident. Program errors can become the training ground for dishonest system users.

COMPUTER VIRUSES

Some applications software packages aren't what they seem. Computer "viruses" (small programs that "infect" computer systems much like biological viruses infect humans) can be hidden in seemingly harmless routines. These viruses can cause extensive data loss or corruption and disrupt your processing operations. In the case of real-time life-dependent systems, the results could be deadly.

Since computer viruses can replicate themselves, they can infect other programs. If software is shared between systems, the virus infection can spread from one system to another.

As with biological viruses, prevention is the best answer. Preventative measures include:

- Don't use copied software. Use only legal, original versions of all computer programs.

- Never use software obtained from public electronic bulletin boards, computer clubs, or similar suspect sources.

- Don't share floppy diskettes casually. If you must transport floppies between systems, make certain they contain only data files, not programs or executable files.

- Don't use computer games. Some of these are known sources of viruses.

- Don't boot systems from a floppy diskette unless recovering from a virus attack. Even then, make certain that the boot diskettes are the original virus-free versions.

- Don't let outsiders use your system without a valid reason and prior approval. You cannot be certain what someone might do to your system, even accidentally.

- Make data backups! This is fundamental to good computing and is also an effective remedy if a virus destroys your primary source of data. Carefully mark backup copies and store them in a safe place.

While viruses have received considerable media attention, preventative measures are generally fairly simple. Unfortunately, these safeguards are often inconvenient, so viruses have had far more impact than they could have.

SOFTWARE PIRACY

A slightly different aspect of software security concerns protecting commercial software. Most software developers copyright these systems and strictly license their use. These licenses usually restrict such things as the number of copies you can make of them and the number of systems on which you can install them. When you buy commercial software, all you are actually purchasing is the right to use that software in accordance with the license restrictions.

Some employees find it difficult to resist the urge to copy licensed word processing, graphics, spread sheet, or other software packages to use on home computers. Strongly inform employees that this kind of casual program copying or "software piracy" is really nothing more than computer program theft. Even though they may return the original copy of the program to its proper place, they have still stolen something. They have stolen a portion of the time and effort the software developer invested in the product.

This unauthorized copying of proprietary software is a special concern. Legal penalties for unauthorized software copying can be as much as $100,000 per incident. Criminal penalties are also possible of up to 5 years in jail.

If you have illegal copies of software, get rid of them! If you need a particular software package, get it legally. Carefully review the license agreement on all software you use and make certain you comply fully.

COMMUNICATIONS CONTROLS

More and more, computer systems are being networked to communicate with each other. When this happens, simple physical protection of data becomes inadequate and communications security becomes necessary.

SYSTEM ACCESS

Beyond the physical access to a computer or terminal, system use is controlled by communications software routines. Most routines allow adjustment of the number of erroneous log-on attempts before the system "locks out" the user. You should configure systems to allow only a very small number of invalid log-on attempts (three or less) before lock out.

When a device has become locked due to invalid log-on attempts, unlock it only after thorough investigation of the circumstances.

DIAL-UP ACCESS

Telephone dial-up access to computer systems poses many control problems. When you attach a telephone communications device (called a modem-modulator/demodulator) to your system, you open your door to virtually the entire world.

Change dial up computer phone lines immediately if you suspect that they've been compromised. Caution all employees about the sensitivity of these telephone numbers.

Be certain to disconnect communications devices when they aren't in use. Carefully check audit trails for communications intrusion attempts.

EFFICIENCY VERSUS SECURITY

To save a few seconds, users will sometimes program a function key on a microcomputer to automatically establish communications with another system. These special routines usually

include telephone numbers, user identification codes, passwords, account names, and similar information. Practices such as this present obvious security problems. Remind employees that efficiency isn't always paramount.

ENCRYPTION

Encryption simply means putting data in a coded form. Without the "key" to the code, the information is meaningless to others. Encryption is an especially effective safeguard against a variety of threats.

Encryption is required for all classified data communication. In some cases, encryption is also required for sensitive unclassified data communication. Talk to an information systems security specialist about your communications encryption requirements.

PERSONNEL SECURITY

Well trained, highly motivated, ethical people are a key safeguard. But remove even one of those characteristics and you have the potential for serious errors, omissions, abuse, and crime.

Statistically, employee misconduct is second only to errors and omissions when accounting for data processing related losses. Computer-related crime and system abuse can take many forms and must be carefully guarded against.

USE CAUTION

Personnel security is one of the most sensitive aspects of security administration. Obviously, high morale is more likely when employees work in an atmosphere of trust and confidence, and low morale may be anticipated when the atmosphere is filled with suspicion. But many computer users are given virtual "keys to the kingdom." Again, you must strike a balance between operational needs and effective control. Don't give employees more power than they need to do their jobs. Divide critical functions among employees whenever possible.

Don't think that because your employees have security clearances that you're immune from personnel problems. One major defense contractor issued 20,000 floppy diskettes to 600 microcomputer users in the space of a few months (do you think maybe they were taking a few home?). Even worse, employees were stealing memory boards from the company's microcomputers to place in their own micro-computers at home. All of this happened at a highly secure facility with cleared employees, so think again about your protective measures.

Employee training is a crucial factor. That may seem obvious, but how often have you been given a task without being given needed training or information? How much do you understand about your information systems?

Some experts estimate that 50 to 80 percent of our problems with automated systems are caused by people whose loyalty and integrity may be beyond question but whose training, judgment, or skill are seriously lacking. In such a technical and complex area, proper instruction is essential. Without it, your error rate can skyrocket.

Other factors can also affect error rates. Subordinates may have problems outside of the job which affect work quality. We are usually reluctant to take action regarding an employee who may have a drinking or drug problem, financial problems, a poor attitude toward work, or other personal problems. It just isn't in our nature to meddle in others' business. If we do get involved, our goal is usually to help the afflicted person. This is generous and admirable but you should also consider revoking or limiting the person's access to your computer systems until the problem is resolved or under control. If you must dismiss an employee, terminate their system access immediately.

TRAINING IS FUNDAMENTAL

In the past, except for a relatively small number of sensitive jobs, the negative effects of poor personnel security were reasonably limited. Today, the power of our computer systems means that one person can have a serious negative impact. Masses of data can be corrupted or destroyed with the push of a button. Sensitive data can be widely distributed, possibly without authorization. Fraud and misappropriation can reach huge proportions. Espionage and sabotage can easily occur. The possible adverse deeds stagger the imagination.

Every employee has the right to a private life, but people entrusted with the capabilities of today's computers must be of the highest caliber. You must monitor your employees in the workplace if you want to protect your vital assets.

MAKE SECURITY EVERYONE'S DUTY

Include security criteria in job performance standards. This is obviously necessary for persons assigned special security responsibilities but it is also a worthwhile measure for any employee who uses a computer. People work hardest at duties on which they are explicitly evaluated.

Including even a simple statement like "Fully and actively supports security efforts" in job standards helps to motivate employees. It shows to them that you take security seriously. It could also give you some leverage in correcting or removing a person who presents a threat to your system.

PROCEDURES

In many respects, procedures are the cornerstone of your total operations and of your information systems security program. In most microcomputer and word processing operations, procedures are virtually the only safeguards available. Effective procedures can prevent or mitigate the effects of routine problems, errors and omissions, and even disasters such as fire, water damage, and so forth. Good procedures can help offset weaknesses in each of the other control areas discussed.

INFORMATION SYSTEMS USUALLY LACK CONTROLS

Automated information systems often reduce the number of controls in the normal operational process. We no longer have the check points, separation of duties, and managerial

reviews that are usually present in manual systems. Automated audit trails are often lacking. Data is concentrated in a few locations.

These problems are particularly noticeable in the microcomputer environment. The microcomputer operator may also be the programmer, the data entry clerk, the media librarian, the output control clerk, and the end user. This is tremendous control and authority to place in the hands of one person.

You need appropriate technical controls and safeguards for your information systems. Protection of files and key data fields within them, reasonableness checks, change summaries, and audit trails (manual or automated) all help to prevent or identify system abuse.

Automate your operation judiciously. Don't abdicate control of your operation in your quest for increased efficiency. A system without effective controls is extremely vulnerable to error and abuse.

PASSWORDS

Passwords are the most widely used way of controlling access to information systems. This makes passwords critical to system protection. A password is proof to the system that a user is who they claim to be and is therefore authorized to use the system. Passwords are only as effective as you and your subordinates make them. Advise users about password sensitivity and security, and hold them strictly accountable for protecting passwords.

DATA BACKUP

Data backup is another important procedural control. This means making frequent copies of the information you process and the programs used to process it.

What would happen to your operations if a hardware failure caused loss of major portions of the data in the system? What would happen if someone accidentally or maliciously erased critical information? What if someone stole a disk or tape that contained information vital to your mission? Routine backup of your data whenever significant changes occur should allow you to continue your operations with little or no delay.

Store backup copies of data (and necessary software and documentation) in a safe place away from the primary copy. That way, anything affecting your primary copy won't also affect your backup copy.

If you are planning for a new computer system, make certain you give adequate thought to data backup capabilities.

MAGNETIC MEDIA CONTROL

Carefully control magnetic storage media such as diskettes, tapes, and hard disks. Mark media externally with the sensitivity of the data on the media, as well as with the contents and the organization and office identification. This will help prevent errors and will alert employees to those items requiring special protection. It could also help ensure the protection and return of lost media.

Consider any magnetic media from outside your organization suspect. Guard carefully against computer viruses.

Strictly control magnetic media leaving the work area. This is often difficult in an office environment but it is nonetheless important. It's possible to remove a small diskette or tape which contains hundreds of pages of information. If an employee walked out with several armfuls of paper, it would be quite noticeable and you'd probably question them. Take care that the same information loss doesn't occur simply because the format is smaller.

PRINTED MEDIA CONTROL

Safeguard system documentation and user guides. These items can serve as a "road map" to your operation and give a system attacker a serious advantage.

Destroy waste products (don't simply trash them) whenever they contain sensitive information. Many abuses of computer systems have occurred because passwords, audit listings, documentation, and other sensitive materials were carelessly thrown away.

OTHER PROCEDURAL SAFEGUARDS

Check occasionally to see that only official work files are on your system and that unnecessary files are deleted. This is one area where security and operational needs go hand in hand. Not only will you reduce your risks by eliminating these files, you free mass storage space for legitimate uses.

Periodically (at least semiannually) inventory equipment, media, software, and other system resources. Expensive but little used items often have a way of disappearing unless locked away or otherwise carefully safeguarded.

CONTINGENCY PLANNING

It's a beautiful autumn morning. The air is cool and fresh. The sun is just beginning to light up the multicolored foliage of the trees. Everything seems right with the world.

Then you open the door to your office.

Disaster! Sometime during the night a fire broke out. Although the building sprinkler system contained the fire, much has been damaged by smoke and heat. And what the fire hasn't destroyed or damaged, the water from the sprinklers has damaged. A sobering scenario, especially if you use and depend heavily upon your information systems. Now what will you do?

The circumstances could be different. The damage could be caused by a leaking roof or overhead water pipe. It may be equipment damage caused by electrical storms. It could even be complete destruction of your building by tornado, earthquake, or other major disaster.

All of these and many other catastrophes have occurred to data centers and still occur with regularity. These kinds of low occurrence/high cost problems are impossible to anticipate exactly, but an attitude of "it won't happen here" is nothing more than managerial negligence.

Information systems become so ingrained in our operations that we become reliant, sometimes totally dependent, upon them. Often once the automated system is in place, we "burn our bridges" and no longer have the capabilities (manpower, time, documents, etc.) to fall back to our previous mode of operation.

So your systems not only need protection, you need contingency plans for processing essential data in case you lose your normal processing capabilities. We call such plans disaster recovery plans or continuity of operations plans. Perhaps we should call them mission continuation plans.

Some continuity of operations plans involve using other compatible systems in your own organization (but in a different location, to avoid one disaster eliminating all systems). Or maybe you'll need a reciprocal agreement with a site using equipment similar to yours.

Continuity planning for small office systems is relatively simple, often simply a matter of substituting less needed systems for the out-of-service but crucial ones. Plans for large systems can be quite complex, however. And planning for alternative processing is only one part of the planning needed for overall resumption of your mission.

Any difficulties in developing a continuity of operations plan are probably minor compared to the potential consequences of operating without one. Costs of contingency planning must be viewed as simply a part of doing business in today's high tech environment.

Give careful thought to your contingency needs. Do it now, before your system is affected. When you have developed your plan, you must test it initially and periodically to ensure its workability.

It isn't a question of if something will happen to your system, but when.

SECURITY AWARENESS TRAINING

There's a story of a museum guide who was just finishing the tour. As the group he was guiding approached the final exhibit he said, "And here, ladies and gentlemen, at the close, is this splendid Greek statue. Note the noble way in which the neck supports the head, the splendid curve of the shoulders. And especially note the natural way in which the open hand is stretched out, as if to emphasize: 'Don't forget a tip for the guide.'

The same idea applies to information systems security training. If we want computer users to act properly, we must instruct them. Anytime you want action, you must let people know what you expect of them.

Since disruption of vital automated information systems could impair Army missions, training the users and managers of those systems has become crucial. Without training, our systems will lack needed protection.

Security training should take three forms: initial, recurring, and final.

Initial training is for newly assigned personnel or to those persons new to using computer equipment. This is a golden opportunity to instill correct behavior. Newcomers usually have few preconceived ideas about their new duties. They have a fresh perspective and their minds are open. Since they are new and security practices are simply part of the job, they take it seriously. This positive attitude results in willing compliance and active support of your security program.

Don't slight the opportunity to start newcomers off right. The tone set now will have lasting effect. Explain briefly the who, what, where, when, and why of security measures. Tailor your instruction to your operations and use real-life examples. Especially explain the why of information systems security; the value of the information at stake, and the potential consequences of security failures.

Give recurring training to system users frequently. Everyone recognizes that a truly important subject is discussed more than once a year. Safety, for example, is discussed on a continuing basis and is stressed even more at holidays.

People assigned to duties involving computer systems - whether they are managers, users, or technical specialists - should receive a steady stream of computer security information. After all, there is a tremendous amount of activity in this field. Considering the diversity of concerns in the field, this is not surprising.

Computer viruses, software piracy, hackers, technical failures, processing disruptions caused by accidents and natural disasters, computer-assisted crime - all these and more regularly make headlines. Take advantage of these events by discussing how they relate to your operations and how computer users can avoid them.

Stress the role each employee plays in creating a positive security environment. Emphasize the importance of being an active participant. Remember also that your personal example tells your followers far more than pious words.

Final security training is for personnel who are leaving the organization or their automation assignment. This is the time to remind them of their continuing responsibilities, especially if they have had access to classified or sensitive unclassified information. This is also the time to change passwords and take other appropriate security actions.

In today's high tech environment, good security training is simply a must. Well-trained and highly-motivated people are, beyond question, the most important safeguard of our automated information systems. Failure to train people in security practices will eventually result in overall failure.

Don't let it be your failure.

MANAGING YOUR COMPUTER SECURITY PROGRAM

As already noted, information systems security depends upon management interest and commitment. Without your active interest and support, your program will fail. Conducting an effective computer security program sometimes calls for special skills.

AR 380-19 is the guiding regulation for Army information systems security efforts. The regulations listed in Appendix B also provide guidance on controls and safeguards for information systems.

Commanders and managers are specifically tasked with information systems security responsibilities. Security specialists or those persons assigned collateral security duties are, for the most part, primarily advisers and administrators.

SYSTEM ACCREDITATION

Every automated information system - including microcomputers - is restricted to operating within the bounds of a specific sensitivity designation. This system sensitivity level is based upon the type of data processed on the system. Sensitivity levels are described in detail in AR 380-19. Take care to ensure that system users understand the approved sensitivity designation for your system and don't exceed that level.

Unless a system has been formally designated "Nonsensitive," the system also requires accreditation. Nonsensitive designations can only be made by the person who would otherwise be the accreditation authority for the system.

Accreditation simply means a formal approval to use the system, based upon a review of several pertinent factors. The accreditation approval is based upon a document which describes the system (its type, configuration, environment, interfaces, etc.), the uses of the system, and the system's threats, vulnerabilities, and safeguards. The accreditation document is submitted to and reviewed by the designated accreditation authority who determines if it is in the Army's best interest to operate the system as described.

Accreditation is required before the system becomes operational. The system then must also be periodically reaccredited.

Designated accreditation authorities are carefully restricted by AR 380-19. Not just anyone can be an accreditation authority. Accreditation is an extremely important effort. Not only does it make it "legal" to operate the system, but the very act of formally identifying vulnerabilities and threats can often lead to the development of important controls.

Note: Any system without current accreditation is subject to suspension of operations without notice.

SECURITY DUTIES

AR 380-19 calls for several special security positions. The Region Information Systems Security Manager (ISSM) directs and coordinates these efforts region-wide. The Region ISSM is located in the First Region (ROTC) Information Management Division and is responsible for establishing guidelines and procedures ensuring the implementation of Army and command regulations, and coordinating information systems security efforts within the region.

An Information Systems Security Officer (ISSO) is appointed at Region/Brigade/Battalion level. In fact, AR 380-19 requires a security chain of command that parallels the operational chain of command. The ISSO is the focal point for information systems security.

Each automated information system needs a System Administrator (SA). These individuals are responsible for keeping the Automated Information System operational and the system secure.

Involve security personnel early in plans for new or changed operations. The best and least expensive security measures are those designed and built into systems from the beginning, not those added on later. Don't let security measures become "band aids" applied to systems only after a problem has occurred.

Give recommendations for enhanced security the same weight you give suggestions to improve your capabilities in other respects.

CONCLUSION

Vital data and programs can be destroyed or damaged, sensitive information revealed, financial loss caused, personal privacy rights violated, serious mission impairments suffered, and negative publicity generated if you don't protect your information systems. All of the advantages your information systems have brought are jeopardized without effective controls. You must act now, before a serious loss or a crisis occurs from which recovery may be difficult or impossible.

It's easy to become preoccupied with the miniature crises of day-to-day operations and with questions of optimal performance from your information systems. This is shortsighted and can lead to considerable problems. You must "balance your scales" and concern yourself with more than just efficiency. You must address the control, safeguard, integrity, and ensured continued availability of your information. Although your systems may then lack that "Nth degree" of efficiency, they will actually be more valuable to YOU.

This FRMOI has presented only the "tip of the iceberg" regarding information systems security but you should now better understand the need for protective measures and what needs to be done. Why not start today? Review your situation and make certain you have effective controls and safeguards for your operations. If you have specific questions about protecting your information systems, talk to the First Region (ROTC) Information Management Division.

Remember, security is a managerial problem. Show your employees your concern by fostering an atmosphere of awareness and good practices. If employees see that you are aware and honestly concerned, chances are that they will mirror your attitude. (Remember, your actions tell your employees far more than do your words). Consider security practices when you evaluate your employees' performance. When employees become actively concerned, your operations will be under much closer and more continuous scrutiny, which will aid security immensely.

Security efforts must include everyone involved: managers, users, and technical specialists. But most important is support from the top. As a manager, you are part of that key support. You are among the top.

Protection of these vital systems is in YOUR hands.

FRMOI 380-3
Appendix A
22 February 2002

SELF-ASSESSMENT CHECKLIST

1. Have you identified all key assets (computer hardware, communication links, sensitive data, etc.) within your area of control?	YES	NO
2. Is each system operated within the bounds of a specific sensitivity designation?	YES	NO
3. Have you conducted valid risk assessments of your systems?	YES	NO
4. Have you implemented effective controls in the following areas:		
a. Physical protection?	YES	NO
b. Software security?	YES	NO
c. Communications controls?	YES	NO
d. Personnel security?	YES	NO
e. Procedures?	YES	NO
f. Contingency planning?	YES	NO
g. Security education?	YES	NO
5. Is security a part of the system's life cycle management?	YES	NO
6. Have people been appointed to security duties - and trained in their specific responsibilities?	YES	NO
7. System accreditation.		
a. Are your systems accredited?	YES	NO
b. Are the accreditations current?	YES	NO
c. Are accreditation documents accurate and thorough?	YES	NO

REFERENCES

This publication has discussed a number of issues pertinent to information systems security. It is an informal document intended to raise your awareness and to serve as a quick reference guide about specific information systems security safeguards.

If you have specific questions or recommendations concerning the protection of the systems you work with, talk to the First Region (ROTC) Information Management Division.

For specific Army policies and requirements, refer to the following:

a. AR 380-19

b. AR 25-1

c. AR 25-55

d. AR 340-21

e. AR 380-5

In addition to this MOI, another is available to help educate users about protection of automated systems. It is FRMOI 380-2, Information System Security - Users Guide.

GLOSSARY

Section I - Abbreviations

FOUO
For Official Use Only

ISSM
Information System Security Manager

ISSO
Information System Security Officer

SA
System Administrator

Section II - Terms

Accreditation
A formal statement by a designated approving authority that appropriate security measures have been implemented for an automated information system and that the level of security risk is acceptable.

Applications software
Computer programs designed to perform specific user-oriented function, such as word processing, spreadsheets, inventory, and so forth.

Audit trail
A record of system activities sufficient to enable review and examination for security purposes.

Countermeasure
Any action, device, procedure, technique, or other measure that reduces the level of risk.

Data integrity
Those aspects of data quality referring to accuracy, completeness, and timeliness.

Sensitive unclassified information
Information which requires protection because its unauthorized loss, disclosure, modification, or destruction could damage government operations or violate legally protected personal privacy.

Stand-alone processing
Processing involving a single user at a time, with no communication with another computer system.

System life cycle
The steps of any computer system's useful span. This includes all aspects (hardware, software, etc.) of the system, from inception and design through controlled dismantling or destruction.

Technical controls
Safeguards which rely on the hardware or software of the computer system in question. These usually require technical specialists for control planning and implementation.

Threat
An activity, agent, or situation - whether accidental or deliberate - with the potential to cause harm.

Vulnerability
A flaw or weakness which can be exploited to cause harm.